Coordinated Load-Changing Attacks on Power Grids

Adrian Dabrowski, Johanna Ulrich, Edgar Weippl

Problem & Motivation

Static Load Attacks
In static load attacks, the adversary synchronously increases the electric load of the bots. The impact on the frequency is shown for a grid with high rotational inertia ($T_s = 10\,s$), i.e., predominantly fed by conventional power plants, and low rotational inertia ($T_s = 6\,s$), i.e., fed by a high share of renewables, at different levels of total network power. Static load attacks are in multiples of the ENTSO-E reference incident (3,000 MW).

Dynamic Load Attacks
In dynamic load attacks, the adversary increases the load to the maximum and waits for the primary control to be activated; then, she decreases the load deactivating primary control again.

Controllable Load
From our own measurements and data sheets, we compiled a table of controllable load by PC components and Internet-of-Things devices encompassing the potential for increasing and/or decreasing power, latencies of power modulation, and the amount of controllable load.

Table 1: Latency and Achievable Load Differences

Conclusion
An adversary does not have to rely on smart grid features to modulate power consumption, given that an adequate communication infrastructure for striking the (legacy) power grid is currently nearly omnipresent: the Internet, to whom more and more power-consuming devices are connected. Our simulations estimate that between 2.5 and 9.8 million connected devices (201-297 W) can be controlled to avert a fail of the European synchronous grid.